

Abstract of the Disclosure:

In the case of cryptographic processing with the aid of an elliptic curve, parameters of the elliptic curve are stored in a memory of a computer. These parameters are each of substantial length. The elliptic curve is transformed in order to shorten at least one parameter significantly in length and to ensure that the high security level is unchanged in the process. One parameter is preferably shortened to 1, -1, 2 or -2 with the aid of an algorithm, whereas the other parameters have a length of several 100 bits. The shortening of even one parameter is clearly reflected in the case of devices which have little memory space.

WHS:tg - 98p1180F//8/14/2000